

UNITED STATES DISTRICT COURT

for the
Eastern District of Pennsylvania

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
Records in re Sprint #610-800-8894,
stored at premises controlled by Sprint

Case No. 17-601-M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment "A," incorporated here

located in the _____ District of _____ Kansas _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment "B," incorporated here.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C Section 111	Assault on federal officers

The application is based on these facts:

See attached affidavit, incorporated here

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Christian Tumolo

Applicant's signature

Christian Tumolo, Deputy U.S. Marshal

Printed name and title

Sworn to before me and signed in my presence.

Date: MAY 3, 2017

DAVID R. STRAWBRIDGE

Judge's signature

City and state: Philadelphia PA

U.S Magistrate Judge DAVID R. STRAWBRIDGE

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF:
RECORDS IN RE SPRINT # 610-800-8894,
STORED AT PREMISES CONTROLLED BY
Sprint.

Case No. 17-601-M

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Christian Tumolo, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Sprint, a wireless provider headquartered at 6480 Sprint Parkway, Overland Park, KS, 66251. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Sprint to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Deputy United States Marshal with the U.S. Marshals Service (USMS), and have been so employed for approximately 13 years. My responsibilities at the USMS include conducting fugitive investigations to locate and apprehend fugitives from justice for Federal, State, and Local criminal violations. My investigations often involve the use of electronically stored data, and in particular, data recovered from cellphone records. I have received specialized training through both the USMS and the Federal Law Enforcement Training

Center in the conduct of criminal investigations during my career as a federal law enforcement officer. Prior to being employed with the USMS, I was employed as both a Federal Police Officer for Veterans Affairs Police and Federal Corrections Officer at the Bureau of Prisons for a total of approximately 3 years.

3. I am the investigator assigned to this investigation. This affidavit is based on, among other things, my training and experience in conducting criminal investigations, my personal knowledge, interviews of witnesses, my review of documents, public records, other evidence, and conversations with other law enforcement agents and officers, including experienced USMS investigators with whom I work. I have not included every fact that I have learned during this investigation, but only sufficient facts to establish probable cause. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 115 have been committed by Mikeamein Foreman. There is also probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B.

PROBABLE CAUSE

4. On November 22, 2016, a warrant for arrest was issued by the Pennsylvania Board of Probation and Parole for Mikeamein Foreman, DOB: 11/13/1989, charging him with violations of his state court supervision. The warrant was issued after Foreman knowingly absconded from supervision at his designated halfway house, located at 1917 W. Oxford St. Philadelphia, PA. After the warrant was issued, Foreman became a fugitive, and the United States Marshal Service Fugitive Task Force undertook an investigation to locate and apprehend him. On 02/16/2017, investigators attempted to locate and apprehend Foreman at numerous

locations which he was known to frequent. One of these was the home of Foreman's mother and sister, 107 W 24th Street Chester, PA, 19103. Investigators visited the residence, and one of them, Task Force Officer (TFO) Michael Gmitter, left Foreman's mother with a business card containing TFO Gmitter's cellphone number. About 15 minutes later, Foreman contacted TFO Gmitter on that number. Foreman called from 610-800-8894; call detail records provided by Sprint pursuant to a court order show that this number belongs to Sprint. There followed a protracted period during which Foreman, using 610-800-8894, communicated with TFO Gmitter by voice calls and text messages about whether Foreman would surrender peacefully. Foreman initially said that he would meet Gmitter and surrender but ultimately reneged on his agreement to do so.

5. On February 16, 2017, federal investigators and local police located Foreman on the 1100 Block of Spruce Street in Chester, Pa, and attempted to arrest him. Foreman fled in a sport utility vehicle, which he used to intentionally ram a vehicle occupied by Deputy U.S. Marshals. Several Deputy Marshals were injured, and their vehicle was damaged. Foreman was eventually arrested after he wrecked his escape vehicle in a separate collision.

6. In my training and experience, I have learned that Sprint is a company that provides cellular telephone access to the general public, and that stored electronic communications, including retrieved and unretrieved voicemail, text, and multimedia messages for Sprint subscribers may be located on the computers of Sprint. Further, I am aware that computers located at Sprint contain information and other stored electronic communications belonging to unrelated third parties.

7. Wireless phone providers often provide their subscribers with voicemail services. In general, a provider will store voicemail messages on behalf of a particular subscriber until the subscriber deletes the voicemail. If the subscriber does not delete the message, the message may remain in the system of Sprint for weeks or months.

8. Among the services commonly offered by wireless phone providers is the capacity to send short text or multimedia messages (photos, audio, or video) from one subscriber's phone or wireless device to another phone or wireless device via one or more wireless providers. This service is often referred to as "Short Message Service" ("SMS") or "Multimedia Messaging Service" ("MMS"), and is often referred to generically as "text messaging." Based on my knowledge and experience, I believe that stored electronic communications, including SMS and MMS messages that have been sent or received by subscribers, may be stored by Sprint for short periods incident to and following their transmission. In addition, providers occasionally retain printouts from original storage of text messages for a particular subscriber's account.

9. Wireless phone providers typically retain certain transactional information about the use of each telephone, voicemail, and text-messaging account on their systems. This information can include log files and messaging logs showing all activity on the account, such as local and long distance telephone connection records, records of session times and durations, lists of all incoming and outgoing telephone numbers or e-mail addresses associated with particular telephone calls, voicemail messages, and text or multimedia messages. Providers may also have information about the dates, times, and methods of connecting associated with every communication in which a particular cellular device was involved

10. Wireless providers may also retain text messaging logs that include specific information about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number (“ESN”), a Mobile Electronic Identity Number (“MEIN”), a Mobile Identification Number (“MIN”), a Subscriber Identity Module (“SIM”), an International Mobile Subscriber Identifier (“IMSI”), or an International Mobile Station Equipment Identity (“IMEI”). When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

11. Many wireless providers retain information about the location in which a particular communication was transmitted or received. This information can include data about which “cell towers” (i.e., antenna towers covering specific geographic areas) received a radio signal from the cellular device and thereby transmitted or received the communication in question.

12. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers’ full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service utilized, the ESN or other unique identifier for the cellular

device associated with the account, the subscribers' Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates, times and sometimes, places, of payments and the means and source of payment (including any credit card or bank account number).

13. In some cases, wireless subscribers may communicate directly with a wireless provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Wireless providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

14. As explained below, information stored at the wireless provider, including that described above, may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the data pertaining to a particular cellular device that is retained by a wireless provider can indicate who has used or controlled the cellular device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, data collected at the time of account sign-up, information relating to account payments, and communications (and the data associated with the

foregoing, such as date and time) may indicate who used or controlled a cellular device at a relevant time. Further, such stored electronic data can show how and when the cellular device and associated cellular service were accessed or used. Such “timeline” information allows investigators to understand the chronological context of cellular device usage, account access, and events relating to the crime under investigation. This “timeline” information may tend to either inculcate or exculpate the cellular device owner. Additionally, information stored by the wireless provider may indicate the geographic location of the cellular device and user at a particular time (e.g., historic cell-site location information; location integrated into an image or video sent via text message to include both metadata and the physical location displayed in an image or video). Last, stored electronic data may provide relevant insight into the state of mind of the cellular device’s owner and/or user as it relates to the offense under investigation. For example, information relating to the cellular device in the possession of the wireless provider may indicate the owner’s motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

15. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Sprint to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

ATTACHMENT A

Property to Be Searched

a. This warrant applies to information associated with 610-800- 8894 that is stored at premises owned, maintained, controlled, or operated by Sprint, a wireless provider headquartered at 6480 Sprint Parkway, Overland Park, KS., 66251, for the time frame November 26, 2016 to February 24, 2017.

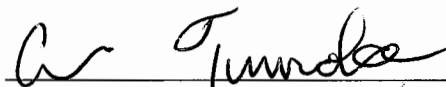
CONCLUSION

16. Based on the forgoing, I request that the Court issue the proposed search warrant. Foreman used the cellular telephone account in question during his flight from law enforcement and evidence of that flight, including his messages to TFO Gmitter, will clearly be contained in the records of the account.

17. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i)

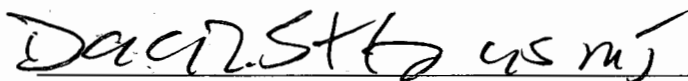
18. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,



Christian Tumolo
Deputy U.S. Marshal
United States Marshals Service

Subscribed and sworn to before me on MAY 3, 2017



HONORABLE DAVID R. STRAWBRIDGE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Sprint

To the extent that the information described in Attachment A is within the possession, custody, or control of Sprint, including any messages, records, files, logs, or information that have been deleted but are still available to Sprint or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Sprint is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. All voice mail, text, and multimedia messages stored and presently contained in, or on behalf of the account or identifier;
- b. All existing printouts from original storage of all of the text messages described above;
- c. All transactional information of all activity of the telephones and/or voicemail accounts described above, including log files, messaging logs, local and long distance telephone connection records, records of session times and durations, dates and times of connecting, methods of connecting, telephone numbers associated with outgoing and incoming calls, cell towers used, and/or locations used from November 26, 2016 to February 24, 2017;
- d. All text messaging logs, including date and time of messages, and identification numbers associated with the handsets sending and receiving the message;
- e. All business records and subscriber information, in any form kept, pertaining to the individual accounts and/or identifiers described above, including subscribers' full names,

addresses, shipping addresses, date account was opened, length of service, the types of service utilized, ESN (Electronic Serial Number) or other unique identifier for the wireless device associated with the account, Social Security number, date of birth, telephone numbers, and other identifiers associated with the account;

f. Detailed billing records, showing all billable calls including outgoing digits, from November 26, 2016 to February 24, 2017;

g. All payment information, including dates and times of payments and means and source of payment (including any credit or bank account number), from November 26, 2016 to February 24, 2017;

h. Incoming and outgoing telephone numbers, from November 26, 2016 to February 24, 2017;

i. All records indicating the services available to subscribers of individual accounts and/or identifiers described above;

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of law including 18 U.S.C. § 111 involving Mikeamein Foreman from November 26, 2016 to February 24, 2017; including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Communications between Foreman and any individuals who may have assisted in his flight from law enforcement; and communications between Foreman, TFO

Gmitter, and any other individuals relevant to Foreman's flight, offers of surrender, negotiations with law enforcement, and the like;

- (b) Evidence indicating how and when the cellular device and associated cellular service was used to determine the chronological context of cellular device use, account access, and events relating to the crime under investigation;
- (c) Evidence indicating the geographic location of the cellular device at times relevant to the investigation;
- (d) Evidence indicating the cellular device owner or user's state of mind as it relates to the crime under investigation;
- (e) The identity of the person(s) who created the account associated with the cellular device and/or used the cellular device, including records that help reveal the whereabouts of such person(s).
- (f) The identity of the person(s) who sent to and/or received communications from the cellular device about matters relating to Foreman's flight from and evasion of law enforcement, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL RULE
OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed Sprint, and my official title is _____. I am a custodian of records for Sprint. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Sprint, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Sprint, and
- c. such records were made by Sprint as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature